REMARKS

The Examiner has maintained the rejection of the claims. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of at least one dependent claim into each of the independent claims. Since the subject matter of such dependent claim(s) was already considered by the Examiner, it is asserted that such claim amendments would not require new search and/or consideration.

The Examiner has rejected Claims 1-5, 8, 10-14, 17, 19-23 and 26 under 35 U.S.C. 102(e) as being anticipated by Bates et al. (U.S. Patent No. 6,785,732). In addition, the Examiner has rejected Claims 6, 9, 15, 18, 24 and 27 under 35 U.S.C. 103(a) as being unpatentable over Bates in view of Hypponen et al. (U.S. Patent No. 2003/0191957). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to at least substantially incorporate the subject matter of dependent Claims 2 and 7 et al.

With respect to each of the independent claims, the Examiner has relied on the following excerpts et al. from Bates to make a prior art showing of applicant's claimed "retrieving code operable to pre-emptively retrieve via said internet link addressed data that would be accessed by a user following said at least one internet address" and "scanning code operable to scan said addressed data for malware" (see the same or similar, but not identical language in each of the independent claims).

> "Virus control mechanism 131 includes the web page virus processing mechanism 132, e-mail virus processing mechanism 134, and file virus processing mechanism 136. Web page virus processing mechanism 132 checks a web client's request for a web page to determine whether the web page or any contained links were the source of a virus in the past." (Col. 5 line 65-Col. 6, line 3)

"...server to automatically check e-mail messages, web pages, and downloaded files for viruses before passing these on to a web client." (Col. 8, lines 1-3)

"If no viruses are found (step 724=NO), and there are no attachments to the e-mail message (step 740=NO), the e-mail message is sent to the recipient (step 714). If a virus is found (step 724=YES), the e-mail message is deleted (step 730), and a separate e-mail is sent to the intended recipient of the e-mail informing the recipient that the deleted e-mail message contained a virus and was automatically deleted (step 732). In addition, any other information regarding the virus-infected e-mail message could be sent to the intended recipient in step 732 as well. Next, method 700 e-mails the sender of the e-mail message that included the virus to inform the sender that they sent a virus (step 734). This step is particularly significant because it prevents a user from repeatedly and unknowingly sending out a virus as part of an e-mail message." (Col. 9, lines 31-45)

First, applicant respectfully asserts that scanning e-mails and files for viruses, in the context taught by Bates, does not meet applicant's specific addressed data. For example, when read in context, applicant's addressed data is that which is "pre-emptively retrieve[d] via said internet link" and "would be accessed by a user following said at least one internet address" (see the same or similar, but not identical language in each of the independent claims). Clearly, the e-mails and files disclosed in Bates are not retrieved via an internet link, as claimed by applicant. In addition, Bates does not disclose that such e-mails or files would be accessed by a user following said at least one internet address, in the manner claimed by applicant. Thus, scanning e-mails and files for viruses does not meet applicant's claimed "scanning code operable to scan said addressed data for malware" (emphasis added).

Second, applicant respectfully asserts that, in Bates, checking web pages for viruses does not include scanning addressable data for malware, in the context claimed by applicant. Specifically, Bates only teaches that "the uniform resource locator (URL) for the web page and for all links on the web page are compared to a list of known URL's in the virus information database 138 that were previously sources for viruses" (Col. 10, lines 58-63). Thus, Bates does not teach scanning addressable data, as applicant claims, but merely comparing a URL with a database of URL's known to have previously contained viruses.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Bates reference, for the reasons noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 2 and 7 et al. into each of the independent claims.

With respect to the subject matter of Claim 2 et al., at least substantially incorporated into each of the independent claims, the Examiner has relied on the following excerpt in Bates to make a prior art showing of applicant's claimed "storing logic operable to store result data identifying at least addressed data in which malware was not found" (see the same or similar, but not identical language in each of the independent claims).

> "The virus information database 138 is a database of virus information that relates to web server computer system 100. Note that virus information database 138 may be a local database, or may be a large centralized database that includes the virus information for many web servers, such as a centralized database that could be accessed via a web site. **Virus information database 138 may include a specification of known viruses, along with statistics for which ones have been encountered and when. In addition, virus information database 138 may include a list of web sites that are known to contain viruses, or from where viruses were downloaded.** A web site that contains a virus or from which a virus was downloaded is referred to herein as a "bad" URL. Using the virus information database 138, web page virus processing mechanism 132 can warn a web client that has requested a web page at a bad URL, or that has requested a web page that includes links to a bad URL." (Col. 6, lines 4-20-emphasis added)

Applicant respectfully asserts that such excerpt merely teaches a database which includes "a specification of known viruses" and "a list of web sites that are known to contain viruses" (see emphasized excerpt above-emphasis added). Clearly, a database that only contains known viruses and websites with known viruses does not meet applicant's specific claim language, namely "storing logic operable to store result data identifying at least addressed data in which malware was not found" (emphasis added).

With respect to the subject matter of Claim 7 et al., at least substantially incorporated into each of the independent claims, the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Bates in view of Razdan et al. (U.S. Patent No. 6,253,301). In particular, the Examiner has relied on the following excerpt from Razdan to make a prior art showing of applicant's claimed technique "wherein said addressed data is cached when it has been retrieved."

> "A page address from a memory address provided by an external probe is compared with a tag read from the duplicate tag array location indexed by the index portion of the memory address. If there is a match, the data addressed by the memory address is currently cached in the data store. Otherwise the output indicates that the addressed data is not currently cached in the data store." (Col. 2, lines 25-30

Applicant respectfully asserts that such excerpt simply teaches that "the data addressed by the memory address is currently cached" (see emphasized excerpt above). Applicant notes however that, in Razdan, only the data from main memory is cached (see Col. 2, lines 15-17). Thus, in Razdan, addressed data is not cached "when it has been retrieved [via said internet link]," in the manner claimed by applicant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the

claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 28-32 below, which are added for full consideration:

"wherein said currently held data is an e-mail and said internet address is an internet link embedded in said e-mail" (see Claim 28);

"wherein said currently held data is a file and said internet address is an internet link embedded in said file" (see Claim 29);

"wherein said malware found actions include removing said at least one internet address from said currently held data" (see Claim 30);

"wherein addressed data determined to contain malware via said scan is cleaned and said clean addressed data is stored locally for access via said internet address" (see Claim 31); and

"wherein access to said addressed data is allowed if said result data associated with said addressed data identifies said addressed data as not containing malware and if said addressed data has not changed since it was last scanned" (see Claim 32).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P475/01.160.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100